TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI
2,00 €
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
n.159
HACKER JOURNAL
www.hackerjournal.it
FATTI LE MAPPE
con il PINGUINO GRATIS
ESCLUSIVA
INTERVISTA AL MITICO
CPT. CRUNCH
LA BAIA VS ITALIA
OSCURATO thepiratebay.org
FRED
il vero ROBOCOP
made in Italy
Spyware, trojan, malware, TRUFFE e le MILLE TRAPPOLE del web
PRONTE AD ESPLODERE
QUATTORD. ANNO 8 - N°159 - 11/24 SETTEMBRE 2008 - € 2,00
WLF PUBLISHING

Anno 8 – N.159
11/24 settembre 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

La **gogna** virtuale

"Ogni giudizio è in bilico sull'orlo dell'errore."
Frank Herbert (1920-1986)

Ho pensato di scrivere questo editoriale due giorni fa e credo di essere alla quinta versione... Ogni volta nuove riflessioni e nuovi punti di vista mi si affacciano alla mente e non riesco davvero a prendere una posizione così preferisco proporvi i miei molti dubbi che le mie pochissime certezze.

C'è un giudice in Nuova Zelanda di nome David Harvey che sta lavorando su un processo per l'omicidio di una ragazzo di 14 anni ucciso da due persone accusate anche di tentata rapina e possesso di armi. Il giudice, che è anche un professore universitario e si occupa di diritto in rete, ha deciso di limitare la diffusione delle immagini e dei nomi dei due accusati ai soli giornali cartacei e al notiziario televisivo della sera, vietando la diffusione di qualsiasi cosa inerente il processo nel web.

D'altro canto c'è una sito negli Stati Uniti chiamato www.nsopr.gov (National Sex Offender Public Registry) dove è possibile vedere la lista di tutte le persone che hanno commesso reati a sfondo sessuale, soprattutto su minori, ed effettuare ricerche per vedere se tra i propri vicini c'è qualcuno potenzialmente pericoloso.

Questi i fatti da cui sono partite le mie riflessioni, ora: se io vivessi negli Stati Uniti con i miei figli e nella villetta affianco alla mia arrivasse un nuovo inquilino probabilmente andrei a vedere se è per caso in quelle liste, d'altro canto mi rendo conto che che il diritto alla privacy deve essere valido per tutti e che una persona che ha pagato il suo debito con la giustizia ha il diritto di rifarsi una vita e, soprattutto, che esistono diversi gradi di "molestia" che possono portare all'iscrizione nelle liste, cioè ad una condanna, e che se una persona ha sbagliato una volta non è detto che debba sbagliare ancora. Inoltre, e mi riferisco qua al caso neozelandese, mi rendo perfettamente conto che la ridondanza della rete e la capacità della stessa di inglobare notizie e mantenerle a disposizione per la gente per molto tempo possa andare ad inficiare il lavoro di una giuria che, una volta convocata potrebbe già essersi fatta dei preconcetti sul caso diffuso in rete.

Insomma, ho tanta confusione in testa come sempre quando si parla di temi così importanti, privacy, sicurezza, libertà d'espressione e d'informazione e via dicendo...

Non so voi, ma io sono lontano dal finire i dubbi, le domande e le riflessioni su queste problematiche, spero vogliate dirmi la vostra a redazione@hackerjournal.it

BigG

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Accoglienza e privacy... FORSE!!!

Si tratterebbe, se i dati venissero confermati, di uno dei più grandi furti di dati mai avvenuti nella rete. Le vittime sarebbero tutti i clienti della catena di hotel Best Western degli ultimi due anni, parliamo di 1.312 alberghi in tutto il mondo per un totale di 86.375 stanze occupate all'anno.
La notizia arriva dall'inglese Sunday Herald, secondo cui un pirata informatico sarebbe riuscito ad installare un trojan su uno dei sistemi di prenotazione utilizzando per impossessarsi degli account dei membri dello staff della catena e poter poi accaparrarsi i dati dei clienti tipo carte di credito, patenti, passaporti e quant'altro.

Tutta questa massa di dati, la stima dei danni si aggira intorno agli 8,2 miliardi di dollari, sarebbe poi stata venduta al miglio offerente attraverso il tristemente noto Russian Business Network.

I dati sono davvero impressionanti e portano questo fatto nelle prime posizioni della mesta classifica dei furti informatici, c'è da dire che la catena di hotel ha risposto ufficialmente all'articolo pubblicato in Inghilterra affermando che la breccia nel loro sistema informatico è di ben più modesta entità e si tratterebbe di una falla in un singolo hotel e non di tutta la rete di alberghi...

Ci spiace molto per la Best Western ma la cosa non ci tranquillizza un gran che, anzi... se ne hanno bucato uno... Comunque c'è molta perplessità sulla rete riguardo il tentativo di ridimensionare il fatto da parte della catena e sembra proprio che, magari non enorme come scritto sopra, ma il danno sia stato davvero grave e quindi consigliamo di buttare un occhio ai propri estratti i conto se si è passati per un albergo della Best Western ultimamente. ■

PALM TREO PRO

Recentemente è stato ufficializzato Palm Treo Pro, uno smartphone completo, con uno stile americano che ha molti fan anche qui da noi nel Vecchio Continente. Rispetto ai modelli precedenti è più curato sotto il profilo estetico, in molti hanno osservato il buon lavoro della Palm. L'azienda a cui era stato commissionato il desiner è la HTC che già aveva raccolto consensi positivi in tutto il mondo per l'ottimo lavoro svolto per Sony Ericsson con il bellissimo X1 Xperia di prossima uscita. Per ora la voce che HTC abbia realizzato Treo Pro è ancora da confermare ma ci sono forti possibilità che non sia solo un rumor estivo. HTC in questi anni ha "donato" la sua esperienza ha tanti altre marche dimostrandosi una delle realtà più solide e concrete del panorama mobile.

MICROSOFT SI ACCORDA PER 100 MIONI DI DOLLARI

Microsoft verserà a Novell 100 milioni di dollari in più. La somma (che costituisce un incremento di oltre il 40% di quanto concordato nel 2006) dovrà essere versata già entro fine ottobre, secondo l'annuncio dato dalle società interessate. Perno dell'accordo sembra sia la promessa "reciproca" che le due software house non si faranno causa per l'eventuale violazione di brevetti; il che ovviamente - se ha tranquillizzato Novell per quanto riguarda la sua versione commerciale di Linux - ha fatto rizzare le orecchie a tutti gli altri produttori dei sistemi operativi open. Alcuni di questi hanno già espresso l'intenzione di stringere accordi con Microsoft, ritenendo di non essere in grado di sostenere le spese legali necessarie per resistere a una causa per violazione di brevetto per inconsistente e fantasiosa che possa essere.

LENOVO W500 E W700 IN ARRIVO

Erano stati presentati qualche settimana fa, finalmente ne è stata annunciata l'imminente spedizione ai rivenditori. Stiamo parlando dei due notebook di Lenovo, W500 e W700, ecco la scheda tecnica con le peculiarità dei due portatili. Lenovo W500 si piazza in una fascia di mercato media, con prezzi che partono da $1,629 per questo notebook con schermo da 15.4 pollici a risoluzione WSXGA+, processore 2.53GHz Intel Core 2 Duo T9400 con 1GB DDR3 Ram, sistema operativo Vista Home Premium, scheda grafica ATI 512MB Mobility FireGL V5700, memoria interna da 100GB HDD, DVD combo drive, WiFi e batteria a 6-cell.
W700, come suggerisce il nome, ha schermo più grande, da 17 pollici a risoluzione e prezzo di partenza più alto, vicino ai 300 dollari, processore T9400 con 2GB di DDR3 RAM, scheda grafica NVIDIA 512MB Quadro FX-2700 e memoria da 160GB.Dovrebbero arrivare presto anche in Italia.

FREEDOM NOT FEAR 2008

Paura di essere sorvegliati, paura di essere catalogati, paura di essere se stessi. C'è chi non intende sprofondare in una spirale del silenzio, c'è chi rivendica il proprio diritto a formare e manifestare spontaneamente il proprio pensiero e la propria creatività: è una chiamata alle armi diramata da Vorratsdatenspeicherung, il gruppo di lavoro che in Germania si oppone alla data retention. Invitano i cittadini di tutto il mondo ad organizzare Freedom Not Fear 2008, Libertà, non paura, una manifestazione globale e decentrata che l'11 ottobre possa scuotere le piazze di tutto il mondo.

UCCIDERE A DISTANZA

Grazie a Kevin Fu, professore associato alla University of Massachusetts Amherst, si è saputo che il protocollo di controllo di questi dispositivi non ha alcuna forma di sicurezza tramite cifratura. Un pacemaker programmabile può essere quindi riprogrammato da un aggressore in modo da somministrare all'utente una scossa elettrica letale. Per farlo basta un apparecchio facil-

I briganti di eBay

Sul sito di aste online più famoso del mondo ci sono molte ottime occasioni. Ma su eBay c'è anche il rischio di incappare in truffatori senza scrupoli. Ecco come riconoscerli e come difendersi. E, già che c'eravamo, abbiamo provato anche noi a diventare "truffatori" su eBay

C'erano una volta i paccari, quelli che ti vendevano le videocamere e i videoregistratori nelle aree di servizio o ai semafori spacciandoli come rubati. E arrivato a casa scoprivi che, sotto le bolle della confezione che ti avevano furtivamente fatto intravedere, i nuovi acquisti erano di legno, con il display dipinto a pennarello rosso e con il cavetto della presa inchiodato dietro. I paccari non è che siano scomparsi: si sono evoluti e usano Internet, tanto i polli da spennare ci sono sempre e si sono trasferiti anche loro lì. E a quanto pare frequentano tutti, truffatori e gabbati, eBay. Sul sito d'aste più famoso e trafficato del mondo, tra le buone occasioni ci sono infatti in agguato anche le fregature. Tra tanta gente onesta che compra e vende, c'è un piccolo ma agguerrito manipolo di persone che tentano il colpo gobbo della piccola truffa. E volte riescono anche a metterlo a segno, anche se spesso vengono "domati" dalla vigilanza lasca di eBay.

◀ *Registrarsi con nome Hacker e cognome Journal su eBay non è stato difficile, fornendo dati completamente falsi. E il codice fiscale? Lo abbiamo ricavato da uno dei tanti siti che permettono di crearne uno partendo da nome, cognome, data e luogo di nascita. Hacker Journal ha codice fiscale JRNHKR61M21F205N.*

:: Come nel mondo reale

Niente di più drammatico che nel mondo reale: i truffatori imperversano su eBay così come ci sono, in mezzo a tanti tranquilli viaggiatori, i borseggiatori sulla metropolitana. O come, tra gli onesti venditori di auto, ci sono quelli che tentano di venderci l'automobile esausta di un commesso viaggiatore spacciandola per quella di un vecchietto che la usava solo per fare la spesa. Normale. Gli annunci regolari su eBay si fiutano subito, così come si possono individuare a colpo d'occhio quelli sospetti. Quelli che, nella vita di tutti i giorni, sono l'equivalente del giubbotto "caduto dal camion" o della telecamera di legno. La truffa più diffusa, ma che non manca di trovare sempre novelle vittime, è quella dei televisori al plasma, delle fotocamere, dei cellulari e dei notebook venduti a prezzi stracciati. Il brigante di eBay si registra fornendo dati falsi, e poi vedremo come in realtà è possibile. Lascia poi "dormire" per qualche mese l'account così creato, per dare l'idea che la sua carriera di venditore non è proprio partita l'altro ieri. E poi si crea qualche decina di feedback fasulli nelle settimane precedenti la frode, comprando oggetti di valore insignificante. Su eBay se ne trovano a migliaia, acquistabili a 0,01 euro o sterline. Di solito libri elettronici o altri prodotti immateriali. In questo modo avrà, spendendo pochissimo, la stella che eBay rilascia dopo dieci transazioni e che dovrebbe essere sinonimo di affidabilità. Ci sono centinaia di annunci che hanno come unico scopo lo scambio dei feedback, non certo quello di comperare o vendere qualcosa.

:: Regole d'oro

La prima regola d'oro è quindi quella di fare clic sul numero di feedback per esaminarli in dettaglio. Se un sedicente venditore si presenta con pochi feedback tutti relativi a prodotti acquistati per pochissimi soldi, e non relativi a vendite, come ci si dovrebbe aspettare da qualcuno che sta vendendo, dobbiamo diffidare. La seconda regola è quella di diffidare delle aste veloci, che durano soltanto tre giorni (una volta duravano anche un solo giorno). Più sono rapide, meno possibilità hanno gli uomini di eBay di accorgersi che c'è qualcosa che non va e di chiuderle prima della chiusura. La terza è di fare attenzione a come il venditore chiede di essere pagato. Il sistema più sicuro per pagare gli oggetti acquistati su eBay è PayPal, assieme ai bonifici bancari e postali. In questo modo non dobbiamo fornire i dati della nostra carta di credito a sconosciuti che potrebbero usarli per altre transazioni. Inoltre, soprattutto se i pagamenti avvengono all'interno della piattaforma eBay, questi sistemi consentono di associare la vendita dell'oggetto con il suo saldo ed è una cosa molto importante in caso di contestazioni. Nelle inserzioni truffaldine di solito non è ben specificato il tipo di pagamento accettato e finita l'asta il venditore spesso chiede all'acquirente un indirizzo di posta personale, proseguendo con le comunicazioni al di fuori di eBay. Fornisce poi il numero di una carta prepagata, invitando a ricaricarla per l'importo della transazione. O chiede di essere pagato mediante Western Union o altri sistemi analoghi per il trasferimento di denaro. Tutti con analoga caratteristica: non sono tracciabili. In pratica non potremo provare che abbiamo fatto noi quella ricarica e nemmeno che è collegata alla transazione. In casi come questi la truffa è certa.

:: I trucchi dei truffatori

Ma come fanno questi truffatori a imperversare su eBay? In qualche caso, tramite tecniche di phishing, rubano password e nome utente di un malcapitato che ha risposto a una di quelle e-mail spazzatura che cercano proprio di carpirti i tuoi dati propro a questo fine. Sono professionisti della truffa e in questo caso difendersi è difficile, perché un account regolare che magari aveva centinaia di feedback tutti positivi, da un momento all'altro passa di mano e viene gestito dal manigoldo. In questo caso non si devono guardare i feedback, visto che il malfattore prenderà tempo con le vittime in modo da raccogliere i feedback negativi solo a truffa finita, ma insospettirsi per offerte troppo convenienti o non coerenti con l'attività precedente del venditore. Se prima ha sempre comperato o venduto libri e ora mette in vendita cento telefoni a 3 euro l'uno c'è da pensare, insomma.

◀ *"Benvenuto Hacker! Sei registrato come utente eBay hackerjournal2008". Sembra quasi una beffa questo messaggio di eBay che ci da il benvenuto come "hacker", anche se in realtà il sito d'aste mette nel benvenuto il nome di battesimo. Che nel nostro caso è proprio Hacker. Ora siamo a tutti gli effetti utenti registrati.*

Immediatamente dopo la registrazione, senza dover spedire nessun documento a eBay, si possono mettere in vendita sino a tre oggetti. Oltre i tre oggetti bisogna provare l'identità a eBay, ma nel frattempo tre tentativi di truffa si possono anche fare. Anche noi iniziamo la procedura per mettere all'asta un oggetto.

eBayAbuse (www.ebayabuse.it) è uno dei tanti siti che conviene frequentare per scoprire quanti e quali sono i truffatori in opera su eBay. Gli altri interessanti sono www.controebay.com, www.antiebay.net e http://truffatoriebay.blogspot.com.

:: Il signor Hacker Journal

Nei casi più frequenti i truffatori si registrano con dati falsi. Non è difficile. Ci abbiamo provato anche noi. In teoria per registraci dobbiamo fornire in nostri dati e il codice fiscale, creando così un profilo con identità certa. Con lo stesso codice fiscale non potremo in pratica creare altri account.

Ma il sistema è facile da aggirare. Abbiamo provato a registrarci come Hacker Journal, nato a Milano il 21 agosto 1961. Il codice fiscale del nostro amico Hacker lo abbiamo ricavato da www.codicefiscale.com. eBay, inserendo il codice fiscale così ricavato e il nickname hackerjournal2008 ci accetta senza discutere: "Complimenti – ci scrive eBay - ora puoi iniziare a comperare e vendere". Possiamo pubblicare immediatamente sino a tre inserzioni di vendita.

Per andare oltre dovremo effettuare la verifica dell'identità, fornendo il numero di carta di credito o un indirizzo fisico a cui eBay spedirà un codice da inserire nel sito. Ma intanto mettiamo un'inserzione in cui vendiamo una copia della nostra rivista a un euro. eBay l'accetta, così come ci ha accettati come venditori anche se in pratica non esistiamo. E cosa ci guadagniamo? Molto, perché come spese di spedizione abbiamo indicato 99 euro. In molti non se ne rendono conto e ci cascano. Chissà che fine farà la nostra inserzione. Quando leggerete questo articolo sarà passato circa un mese dalla registrazione.

Provate a cercarci con il nome utente hackerjournal per vedere se eBay si è finalmente accorta che qualcosa non andava. E controllate se l'inserzione 180274111647 INCLUDEPICTURE "http://pics.ebaystatic.com/aw/pics/globalAssets/rtCurve.gif" * MERGEFORMATINET è stata rimossa, o se è ancora in archivio come chiusa.

Ed ecco la nostra inserzione online, passata su eBay senza tante storie. Vendiamo una copia di Hacker Journal a un solo euro di base d'asta. E il guadagno dov'è?
Beh, se qualcuno la compera senza guardare bene ci porteremo a casa cento euro. Perché le spese di spedizione che abbiano indicato nell'annuncio son di ben 99 euro.

Moreno Soppelsa

FURTO DI DATI PRIVATI: CAPITA SOLO AGLI ALTRI?

Le università americane sono nel mirino dei pirati. Dal gennaio 2008 non è trascorsa una sola settimana senza che si verificassero furti o sottrazioni di informazioni private e dati sensibili di studenti e professori. Inquietante!

Mentre alcune università americane tolgono la connessione a Internet agli studenti che indulgono eccessivamente nello scaricamento di musica, quelle stesse università sembrano dimenticare un aspetto importante di Internet: la sorveglianza adeguata delle loro porte di accesso. Da diverse settimane, non passa giorno senza che ci sia un allarme informatico. I pirati hanno capito che nei server delle scuole dello zio Sam è possibile trovare ben altro che appunti e informazioni sui corsi. Per esempio, dati confidenziali come i numeri della Social Security, che fanno le veci di carta d'identità, codice fiscale e molto altro. Con questo numero è possibile tra l'altro aprire un conto bancario e ottenere il rimborso di tasse pagate in eccesso... insomma, è uno strumento perfetto per un malintenzionato che desideri impadronirsi di un'identità altrui.

Il primo premio della vulnerabilità spetta all'Università della California, che ha già al suo attivo numerosi atti di pirateria tra cui un furto destinato a rimanere negli annali: 800.000 dossier di studenti "prelevati" in un solo anno. Grazie alla stampa americana abbiamo potuto rilevare ben 96 casi del genere, solo nel primo trimestre del 2008. L'ultimo in ordine di tempo si è verificato lo scorso aprile: l'università di Antioch (Ohio) ha "perso" 70.000 dati relativi agli studenti e al personale scolastico. Dall'università statale dell'Oklahoma è stato sottratto un numero analogo di dossier. Il pirata si era infiltrato attraverso il server di gestione del parcheggio dell'istituto. Perfino la prestigiosa università privata di Harvard ha subito un'effrazione. In febbraio, un pirata ha diffuso tramite P2P ben 125 MB di dati di proprietà della scuola.

Il dato più sconcertante è che la polizia federale americana aveva incitato i presidi universitari a trasformarsi negli occhi e nelle orecchie dello zio Sam per contrastare... terroristi e spie. Il comitato consultivo per l'istruzione superiore della Sicurezza Nazionale (National Security Higher Education Advisory Board), costituitosi nel 2005 (http://www.fbi.gov/pressrel/pressrel05/highed091505.htm), è composto da una ventina di presidi universitari di tutto il Paese. I suoi responsabili collaborano con l'FBI su questioni legate alla sicurezza dei campus, al contro-terrorismo e nell'individuare eventuali spie e reclutatori. Secondo il rapporto dell'NPR (http://www.npr.org/templates/story/story.php?storyId=16067492), l'FBI consiglia ai membri del comitato di ragionare come ai tempi della Guerra Fredda. Ai responsabili viene suggerito di sorvegliare professori e studenti sospettati di frequentare il campus a fini di spionaggio o allo scopo di reclutare studenti sostenitori di cause "anti-americane". A prima vista, si direbbe che ci sia ancora molto lavoro da fare!

:: Porte aperte all'università

In marzo, l'università di Ginevra (Svizzera) ha rilevato una fuga di dati relativi a futuri studenti della facoltà di teologia. Fortunatamente per l'istituto, un hacker è passato di lì e ha dato una mano a eliminare il "bug" che consentiva di intercettare nomi, indirizzi e numeri telefonici degli studenti. Anche in Francia ci sono stati problemi analoghi. La Sorbona ha subito attacchi di pirateria nel 2006 a opera di un hacker che operava sotto lo pseudonimo di Furtivo (Xtech Crew). Lo stesso problema si è verificato all'università Claude Bernard di Lione: accesso ai dati privati dei nuovi e vecchi iscritti. Informati, i responsabili della facoltà hanno rapidamente eliminato la falla. In Italia, il problema non c'è o non è ancora stato individuato?

GLI ACCHIAPPA CRACKER

Hacker Journal è andato a vedere come operano gli uomini del Gruppo repressione frodi del nucleo regionale della polizia tributaria della Lombardia

Mettiamo che un cracker, il lato oscuro e criminoso dell'hacker, sia davanti al computer concentrato sull'exploit della notte. Che sia alle prese con un defacement di un sito o lo svuotamento di un conto corrente, la sua paura più recondita è che arrivino le forze dell'ordine, dalla postale alla tributaria. Non guardano in faccia nessuno: entrano con la velocità della luce e la prima cosa che fanno è "congelare" l'hard disk del cracker nello stato in cui si trova al momento della perquisizione, in modo che diventi una prova che in tribunale non possa essere contestata. E' una bella battaglia quella tra chi ha qualcosa da nascondere nel computer di casa o dell'ufficio e le forze dell'ordine. Fatta di esperti informatici, da una e dall'altra parte, tecniche investigative, strumenti sofisticati per setacciare gli hard disk, e una buona dose di psicologia da poliziotto. Hacker Journal è andato a vedere come si muovono, e con quali strumenti, gli uomini del Gruppo repressione frodi del nucleo regionale della polizia tributaria della Lombardia. E ad esplorare una disciplina estremamente interessante, anche se poco alla ribalta delle cronache: la computer forensics.

:: Il forno è un classico

Un classico dei criminali informatici è il forno a micro onde a portata di mano, pronto per essere usato per "cuocere" i DVD e i CD quando la polizia bussa alla porta. Ma gli uomini della Polizia Tributaria con cui abbiamo parlato non si scompongono. Sanno che i dati presenti nel DVD che è stato cotto nel forno non sono più recuperabili da nessuno mentre un hard disk può essere letto anche dopo una decina di formattazioni, ma sanno anche che i dati presenti nei supporti ottici cotti, prima di essere stati inseriti nel DVD, erano sicuramente in un hard disk locale o virtuale. E visto che molto difficilmente dati tanto importanti vengono bruciati senza che ci siano copie in giro, da qualche parte forse ci sono ancora: basta cercare bene. "Certo è che, se quando entriamo vediamo un microonde fumante, cominciamo a pensare male. E a cercare meglio" dicono quelli della tributaria.

:: La computer forensics

E' l'arte della "computer forensics", quella disciplina che si occupa della preservazione, dell'identificazione e dello studio dei sistemi informativi al fine di evidenziare prove per scopi di indagine. Non è facile, perché una prova deve essere acquisita e mantenuta inalterata sino ai vari gradi di giudizio. E basta accendere un computer perché

decine di file di sistema cambino, pregiudicando lo stato della prova. Come la volta, secondo quanto ci ha raccontato un magistrato che ovviamente non vuole essere citato, che il responsabile di un squadra di una forza dell'ordine ha scritto il verbale di perquisizione usando il computer che poi avrebbe dovuto acquisire come prova.
E gli uomini della tributaria infatti non toccano i computer. Nei casi più gravi si portano via gli hard disk e li affidano a FRED. Acronimo di Forensic Recovery of Evidence Device, è una potentissima stazione di lavoro che consente di acquisire e analizzare il contenuto di un disco rigido senza alterarne il contenuto. Nelle foto di queste pagine vedete quella operativa negli uffici di Milano del Gruppo repressione frodi della polizia tributaria. Ha quattro processori, alloggiamenti per hard disk IDE, SATA e SCSI, capacità di memorizzazione di 2,8 TB e una serie di programmi in dotazione per bloccare gli hard disk esaminati, rintracciare i file cancellati, recuperare i dati formattati e così via. FRED è stato sviluppato da Digital Ingelligence (http://www.digitalintelligence.com/products/fredsr).

:: FRED in rete

FRED, nel comando regionale della polizia tributaria della Lombardia, è collegato in rete con le centinaia di computer della sede. Sfrutta la potenza di calcolo di questi computer, nei loro momenti di inattività, per decrittare file e scovare password. "In molti casi – spiegano gli investigatori – non riusciamo comunque a decrittare file o trovare password particolarmente ostiche, ma trovare file di questo genere in un computer ci mette in allarme. Chiediamo all'indagato cosa ci sia in quei file e, in caso di risposte evasive, sarà il magistrato a decidere se approfondire l'indagine rivolgendosi a laboratori specializzati". Una questione di costi e di importanza dei dati da recuperare, insomma. Per un'indagine critica si può ricorrere anche a tecnologie, costosissime, che recuperano dati anche dopo la decima formattazione. Ma se non si tratta, per dire, di spionaggio militare ma di un ragazzino che protegge l'elenco dei suoi Mp3 con crittografia a 128 bit, il gioco non vale la candela. La prima cosa che fanno è comunque quella di controllare i programmi che ci sono nell'hard disk e se gli investigatori trovano software di crittografia o per la steganografia ovviamente fanno un controllo più approfondito sui file.

Un agente investigativo Gruppo repressione frodi del nucleo regionale della polizia tributaria della Lombardia controlla la rete alla ricerca di possibili reati informatici.

:: Altri strumenti

Se le forse dell'ordine non possono o non vogliono portarsi via gli hard disk per passarli al setaccio di FRED, ci sono altri strumenti utili. Come Logicube Forensic MD5 (www.logicubeforensics.com/products/hd_duplication/md5.asp), un aggeggio in grado di clonare un hard disk senza rimuoverlo dalla sua sede alla velocità di 3 GB al minuto. Anche questo strumento è stato fotografato da Hacker Journal e lo potete vedere in queste pagine. I disco viene copiato bit per bit e alla copia viene applicata una sorta di firma digitale, MD5 o Digital Hash, che garantisce nel tempo il fatto che la copia non sia stata in alcun modo alterata. Dal punto di vista del software di analisi, il più utilizzato dalle forze dell'ordine in tutto il mondo, e anche in Italia, è EnCase Forensic di Guidance Software. Acquisisce il contenuto di un hard disk in maniera non invasiva, senza cioè alterare in nessun modo i dati presenti, producendo un esatto duplicato binario dei dati originali. Tra i suoi tool è particolarmente efficace, o pericoloso a seconda dei punti di vista, quello che consente a volte di recuperare anche i file cancellati con Eraser (http://www.tolvanen.com/eraser/download.shtml), un tool di sicurezza avanzato open source che permette di cancellare in modo teoricamente irrecuperabili i dati memorizzati su disco.

Se avrete occasione di vedere questa valigetta da vicino, e soprattutto con il contenuto in funzione, allora vuol dire che siete nei guai. Perché si tratta di Logicube Forensic MD5 (www.logicubeforensics.com/products/hd_duplication/md5.asp), un aggeggio in grado di clonare un hard disk senza rimuoverlo dalla sua sede alla velocità di 3 GB al minuto.

:: Tutti investigatori

Vogliamo provare anche noi a fare della computer forensic? Inutile cercare EnCase Forensic, che non è disponibile sul mercato, mentre la versione per aziende, meno potente, è comunque costosa. Per cominciare alla grande senza spendere nulla possiamo invece scaricare Helix (www.e-fense.com/helix), il live CD basato su Knoppix e strutturato in modo da offrire una serie di strumenti formidabili per tutte le analisi investigative, dall'ispezione di un computer Windows con decine tool open source e freeware, al boot da CD per disporre di un ambiente Linux dedicato attraverso il quale analizzare dischi ed immagini. ■

UN SITO PER COMINCIARE

Possiamo incominciare ad apprendere i rudimenti di computer forenics su www.cybercrimes.it, sito creato da Maurizio Anconelli e Massimo Adduci, esperti in indagini informatiche.

IL BACKUP DEI PROPRI DATI SI EFFETTUA ONLINE

Conveniente, pratico e semplice da utilizzare: sono i principali punti di forza di Memopal, software di backup e storage online, che consente di disporre e gestire i file archiviati da qualunque computer con accesso a Internet

Lo spazio sull'hard disk si va inesorabilmente esaurendo? Dobbiamo partire per un lungo viaggio e vogliamo fare a meno di mettere in valigia il costoso, e magari pesante, disco portatile dove abbiamo archiviato file che potremmo dover utilizzare una volta lontani dal nostro computer? Il problema si risolve con estrema facilità: basta iscriversi a uno dei servizi offerti da Memopal, startup europea che tramite il proprio sito web permette di scaricare un software di backup e storage online che archivia i file in tempo reale su un server remoto.
I nostri file, una volta archiviati online, in maniera sicura, potranno così essere visualizzati e gestiti da qualunque computer collegato a Internet e fornito di browser. Le soluzioni proposte da Memopal comprendono una versione Personal, per l'archiviazione di documenti, email e foto fino a un massimo di 150 Gbyte al prezzo di 49,00 € l'anno, e la più completa versione Business, progettata per un utilizzo professionale, che include applicazioni server e desktop multiutente. In questo caso il servizio è configurabile in base alle specifiche esigenze, quali il numero di utenti, i Gygabite utilizzabili, la durata del servizio stesso e via dicendo. Ad esempio, la soluzione per 4 utenti con uno spazio di 400 Gbyte a disposizione, per la durata di un anno, costa in tutto 1.056,00 €, ossia 264,00 € per utente. Prima dell'eventuale acquisto, è tuttavia possibile provare gratuitamente i servizi di Memopal per un periodo di sette giorni e per un totale di spazio a disposizione pari a 1 Gbyte per la versione Personal, collegandosi alla homepage www.memopal.com, come riportato nella **Fig. 1**, e seguendo le apposite indicazioni.

1

:: Come usufruire del periodo di prova gratuita

Dalla homepage si può accedere alle informazioni sui vari servizi offerti da Memopal. Facendo clic sul link prova gratuita relativo, ad esempio, alla versione Personal, si accede alla pagina di download del software, da scegliere fra le versioni per Windows XP, Vista, o la beta per Mac. Presto, come riportato nelle informazioni sottostanti, dovrebbe essere disponibile anche Memopal per Linux. Scarichiamo dunque il file di Setup, dalle dimensioni di circa 25 Mbyte, salvandolo sul nostro computer, come riportato nella **Fig. 2**.
Una volta scaricato, come recitano le istruzioni della pagina di download, il software va installato, e a quel punto sarà possibile scegliere quali cartelle del computer proteggere. Si procede dunque con l'installazione aprendo il file di Setup scaricato, e si seguono le comuni istruzioni riportate nella finestra di dialogo, confermando i vari passi.

Alla fine della procedura, E' possibile avviare direttamente l'applicazione mantenendo l'apposito flag nella finestra di chiusura dell'installazione.

2

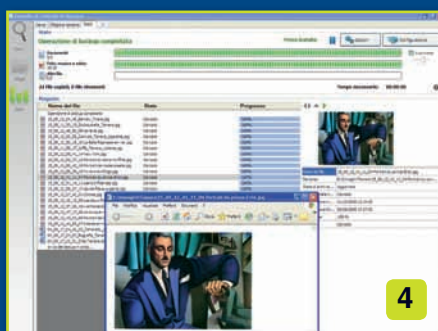
:: Registrazione e configurazione del servizio

A questo punto si apre la finestra per la procedura guidata della configurazione. Una volta selezionato il linguaggio, è necessario registrarsi indicando un indirizzo email e creando una password personale. Una volta confermati i dati, si passa alla finestra successiva, che richiede una particolare attenzione poiché consente di selezionare quali aree del computer sottoporre al backup online, scegliendo fra Documenti (opzione peraltro consigliata dal sistema, che consente di archiviare tutti i file delle cartelle Desktop e Documenti, Email e Dati Applicazioni), Singola Cartella, Tutto il Sistema e Fatta su Misura. Quest'ultima opzione permette di selezionare le cartelle da copiare, offrendo così un alto livello di personalizzazione. Selezionandola, si apre sulla destra il riquadro di esplorazione delle risorse in cui è possibile scegliere gli elementi da sottoporre al backup, come riportato in Fig. 3.

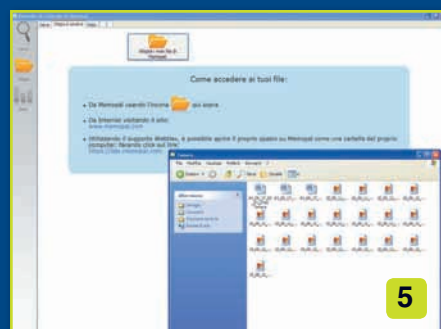
3

:: Attivazione del backup

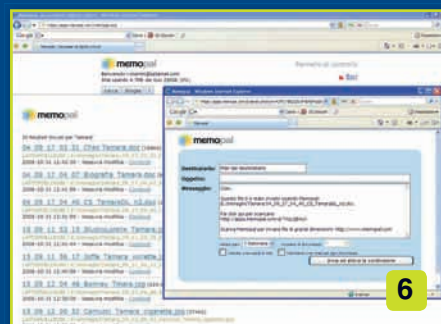
Terminata la procedura di configurazione, il programma avvia l'analisi del computer inviando le cartelle i file selezionati al server Memopal per la memorizzazione sicura. Per controllare lo stato della procedura, che agisce in background, si può fare clic sull'icona posta in basso nella barra delle applicazioni, attivando così il pannello di controllo del servizio. Da qui è possibile gestire tutte le informazioni necessarie relative ai file caricati. Se facciamo clic, ad esempio, su una delle fotografie memorizzate online (nel nostro caso delle riproduzioni degli splendidi dipinti di Tamara De Limpicka), sulla destra del pannello verrà visualizzata un'anteprima dell'immagine con tutti i dati relativi al file, al suo stato (caricato, aggiornato e via dicendo) e alla data dell'ultima archiviazione. Facendo doppio clic, il file viene aperto all'interno di una nuova pagina web, come si può vedere in Fig. 4.

4

:: Come accedere ai propri file

Dal pannello di controllo è inoltre possibile accedere al motore di ricerca di una specifica cartella o file e alla funzione Sfoglia e Ripristina. Nella schermata relativa a tale funzione, vengono riportate le indicazioni per accedere ai propri file, dunque utilizzando l'apposita icona posta in alto, da Internet attraverso il sito Memopal o utilizzando il supporto WebDay, che consente di aprire uno spazio su Memopal come una cartella del proprio computer, facendo clic sul link https://dav.memopal.com. In questo caso si aprirà una finestra in cui digitare il nome utente (corrispondente alla email inserita in precedenza) e la password per avere accesso alla pagina degli elementi archiviati, come riportato in Fig. 5.

5

:: Accesso dal Web e condivisione o invio dei file

Anche la procedura di accesso via Internet è molto semplice, e si effettua tramite l'inserimento dell'ID e della password relativi al proprio account. Un'altra funzione interessante di Memopal consiste nella possibilità di condividere, o inviare senza la necessità di un client email, file di grandi dimensioni, fino a 1 Gbyte. Dal pannello di controllo del sito, molto più semplificato rispetto a quello attivo sul nostro computer, si può ad esempio andare a ricercare un file specifico digitandone il nome per esteso, o in parte, nella casella del motore di ricerca. La schermata successiva indicherà i risultati della ricerca, riportando anche sotto forma di link il comando per la condivisione del file. Facendo clic su di esso si apre una finestra simile a quelle di molti client di posta elettronica online, in cui inserire l'indirizzo email del destinatario, l'oggetto del messaggio e l'eventuale testo di accompagnamento, come riportato in Fig. 6. ■

6

Le mille trappole del Web

Virus e spyware hanno cambiato strategia. Scopriamo quando possono aggredirci e come difenderci

L'epoca dei virus allegati alla posta elettronica è finita. Oggi i pirati informatici usano strategie diverse e sono in grado di colpirci proprio quando ci sentiamo più al sicuro. Per scoprire quali sono i veri pericoli sul Web siamo andati in Germania a visitare la sede di GData, www.gdata.de/portal/IT e abbiamo messo sotto torchio i loro esperti. Il risultato è una panoramica di tutto quello che ci può succedere quando usiamo il computer su Internet.

:: La posta elettronica

Non lasciamoci ingannare: anche se continuiamo a trovare qualche virus allegato ai messaggi di posta elettronica, questa tecnica di diffusione è ormai superata. I worm ancora in circolazione sono in realtà dei superstiti, diffusi addirittura 3 o 4 anni fa. Se sono ancora in circolazione è solo grazie all'incoscienza di quegli utenti che si ostinano a lavorare con un computer privo di qualsiasi protezione.
Questo non significa che i messaggi di posta elettronica non nascondano delle insidie. Tralasciando il semplice spam e i tentativi di phishing, la maggiore minaccia è rappresentata dai collegamenti Internet inseriti nel testo dei messaggi. L'uso di un link al posto dell'allegato, infatti, offre ai pirati informatici numerosi vantaggi. Per prima cosa è molto più facile "convincere" la potenziale vittima a fare clic su un collegamento piuttosto che ad aprire un allegato. In secondo luogo, questa strategia permette di aggirare più facilmente il controllo dei programmi antivirus.

:: Il fattore tempo

I collegamenti pericolosi all'interno delle email sono di due tipi: i più semplici avviano il download di un file tramite il nostro browser, al cui interno si nasconde il virus. Se abbiamo un antivirus aggiornato, ci sono buone possibilità che riesca a identificare il pericolo, ma non possiamo averne la certezza. A differenza di quanto avveniva quando i virus venivano trasmessi in allegato ai messaggi, infatti, la circolazione con questa modalità è molto più rapida ed è sempre possibile ricevere il messaggio ancora prima che i laboratori antivirus abbiano avuto la possibilità di analizzare e catalogare il virus in questione.
Il secondo tipo di collegamento,

invece, "punta" a siti che integrano un codice attivo, molto spesso Javascript, in grado di sfruttare le vulnerabilità del nostro browser e attaccare il sistema senza che sia necessario scaricare e avviare un file eseguibile. In questi casi, la migliore contromisura è rappresentata dal livello di aggiornamento dei programmi che usiamo. Se abbiamo installato la versione più recente del browser e di tutti i plug-in, come Flash e Java, le probabilità di essere colpiti da un virus calano drasticamente.

:: Navigare sul Web

La navigazione su Internet è stata sempre considerata una delle attività più sicure. Le cose, però, non stanno più così. Lo spauracchio di naviganti ed esperti di sicurezza si chiama XSS, o Cross Site Scripting. Si tratta di una tecnica che sfrutta le vulnerabilità dei siti Web per eseguire codice in background, ovvero senza che l'utilizzatore del computer possa accorgersi di nulla. Gli attacchi XSS sono efficaci solo a determinate condizioni: il sito deve contenere uno spazio, per esempio un form per l'invio di messaggi, nel quale sia possibile immettere testo. In secondo luogo, è necessario che il testo immesso venga visualizzato in una pagina Web interna al sito. Infine, il server che ospita il sito stesso, deve essere vulnerabile a questo tipo di attacchi. L'ultima condizione, purtroppo, si verifica spesso. Sono molto pochi, infatti, i server Web che integrano un sistema di filtri per individuare possibili attacchi XSS.
La tecnica, tutto sommato, è piuttosto semplice: il pirata di turno sfrutta il form per immettere le righe di codice Javascript che ha preparato. In teoria, il testo immesso dovrebbe semplicemente essere visualizzato, ma quando il browser "riconosce" le istruzioni le esegue esattamente come se si trattasse di un programma. Attraverso questa tecnica, un pirata informatico sufficientemente abile può compiere qualsiasi tipo di azione.
I siti maggiormente a rischio, in questo caso, sono i cosiddetti Social Network, come MySpace, Facebook e simili. In questi siti, infatti, sono previsti numerosi strumenti che consentono ai visitatori di immettere testi e messaggi per comunicare tra gli iscritti. Una vera pacchia per un pirata informatico intenzionato a portare un attacco XSS.

Nessun allegato, ma un invito a guardare un video su Youtube. L'email, però, è falsa e il collegamento conduce a una pagina Web in grado di infettare il nostro PC con un virus.

L'ESPERTO

La nostra guida è Ralf Benzmüller, responsabile dei laboratori GData in Germania, che ci ha fornito dati e informazioni. Non stupiamoci, quindi, se molte delle immagini riportate nell'articolo sono in lingua tedesca.

:: Ricerche pericolose

Una variante di questa tecnica permette di colpire i siti che contengono una casella per le ricerche online. In questo caso, il Javascript viene inserito direttamente nell'indirizzo di una pagina Web che viene pubblicata su Internet. Nella creazione della pagina, il pirata informatico ha cura di inserire parole e argomenti attraenti. A soffrire di questa vulnerabilità sono i siti che integrano una casella per la ricerca su Internet, magari collegata a un motore di ricerca indipendente come Google o Yahoo!. Sotto un profilo squisitamente tecnico, il funzionamento è identico al caso precedente: quando l'indirizzo viene visualizzato, il browser riconosce il codice e lo esegue.

L'uso di XSS consente di portare due tipi di attacchi. In primo luogo è possibile modificare l'aspetto di un sito, effettuando un defacing, ovvero una cambiamento della"faccia" delle pagine Web. In alternativa, è possibile fare in modo che il codice inserito agisca direttamente sul computer dei visitatori, provocando danni ben più gravi.

:: Anche le pubblicità

I dati raccolti da GData parlano chiaro: nell'85% dei casi, i virus sul Web si trovano all'interno di siti Internet perfettamente legali. I pirati informatici, infatti, preferiscono evitare di pubblicare in prima persona il sito che ospiterà il virus. Una simile tattica, infatti, li esporrebbe troppo e li metterebbe nella condizione di essere rintracciati con facilità. I "cattivi ragazzi" preferiscono quindi usare siti Web già esistenti, meglio se famosi e molto frequentati, inquinandone le pagine dall'esterno.
Una delle tecniche più usate è quella degli iFrame, ovvero di sezioni della pagina Web il cui contenuto proviene da altri server e sui quali è più difficile esercitare uno stretto controllo. L'esempio più significativo è quello delle pubblicità inserite nelle pagine Web. Sempre più spesso, infatti, la pubblicazione dei banner pubblicitari non viene gestita direttamente da chi amministra il sito, ma affidata a una concessionaria esterna. Il webmaster, quindi, non ha alcun controllo sul contenuto delle pubblicità. Ai pirati basta "contaminare" il server che gestisce i messaggi pubblicitari per trasformare decine di siti Internet in una trappola micidiale, in grado di attaccare migliaia di computer in pochi minuti.
Molti browser integrano strumenti per bloccare la visualizzazione dei contenuti pubblicitari. Sebbene siano pensati per "ripulire" le pagine da testo inutile o fastidioso, possono rappresentare un eccellente strumento per la nostra sicurezza.

:: Download dal Web

Scaricare file da siti Internet comporta sempre qualche rischio. Di solito, comunque, basta un po' di buon senso per evitare di cadere vittima di un virus. La pericolosità, tuttavia, deriva dalle tecniche di ingegneria sociale usate dai pirati informatici. Per convincere le potenziali vittime a scaricare file pericolosi, infatti, vengono usate strategie anche molto elaborate, che fanno leva sulla curiosità o sulla paura. Una tecnica molto in voga riguarda i video disponibili online. La visualizzazione in streaming dei video, infatti, è in linea di massima una procedura innocua. I pirati allettano i visitatori del sito promettendo filmati particolarmente interessanti, ma al momento della visualizzazione lo schermo rimane nero e compare un messaggio che segnala un problema nella visualizzazione dovuto ai codec video. Deluso e irritato dal contrattempo, il visitatore nota sulla stessa pagina un collegamento per il download dei codec e si lancia nella procedura d'installazione senza pensarci due volte. Naturalmente, il software che sta per scaricare è in realtà un virus.
Una tecnica simile sfrutta invece la paura per l'infezione da parte di virus e spyware. L'esca, in questo caso, è un falso software online per il rilevamento degli spyware, che indica la presenza di uno o più programmi pericolosi sul nostro PC. Una volta creato il panico, il software propone una procedura per eliminare i presunti virus. Per farlo, però, è necessario installare una versione più potente del software, spesso a pagamento. In alcuni casi, a questo punto, il programma richiede l'installazione e l'aggiornamento.

:: Formati pericolosi

Anche i contenuti attivi e i documenti integrati nelle pagine Web possono rappresentare un pericolo per la nostra sicurezza. Basta pensare al formato Flash, usato molto spesso per pubblicare videogiochi o visualizzare video in linea. Nei mesi scorsi Adobe ha dovuto rilasciare in tutta fretta un aggiornamento dei plug-in Flash proprio a causa di una falla di sicurezza.
Lo stesso discorso vale per i file in formato PDF, sempre più usati per pubblicare su Internet documenti e manuali. Il PDF, infatti, supporta il linguaggio Java e rappresenta un potenziale pericolo per il nostro computer. Anche se in teoria l'esecuzione del codice è "costretta" all'interno del documento, non si può escludere che questa limitazione venga superata da un pirata particolarmente abile. La situazione, poi, è destinata a complicarsi quando comincerà a diffondersi il nuovo Acrobat 9, che supporta nativamente Flash e consente di inserire un gran numero di file ed elementi attivi all'interno dei documenti PDF. Possiamo solo sperare che, con simili cambiamenti, anche i sistemi di sicurezza del formato siano stati potenziati adeguatamente. In questo caso, la migliore strategia di difesa è sempre quella di verifi-

ISOLARE IL BROWSER

Per contrastare gli attacchi sul Web, la prima precauzione che possiamo usare è quella di controllare di avere sempre la versione più aggiornata del browser e di tutti i componenti aggiuntivi. Se vogliamo navigare in condizioni di assoluta sicurezza, però, possiamo scegliere di usare una sandbox, per esempio SafeSpace, http://www.artificialdynamics.co.uk.Si tratta di un particolare programma che isola il browser dal resto del sistema in modo che l'eventuale codice pericoloso visualizzato sul Web non possa modificare le impostazioni del nostro sistema o installare un virus. Teniamo presente, però, che questo tipo di protezione non offre una sicurezza assoluta. Se sul nostro sistema è installato un trojan, per esempio, le informazioni che trasmettiamo sul Web possono comunque essere intercettate. Questo rischio si riduce quando usiamo una connessione crittografata, per esempio tramite il protocollo HTTPS usato normalmente dai servizi bancari online.

care con regolarità gli aggiornamenti disponibili per i software e i plug-in che consentono la visualizzazione dei documenti nel nostro browser.

:: Messenger

I programmi per i messaggi istantanei su Internet rappresentano un veicolo perfetto per virus e programmi pericolosi. Tramite questi software è possibile inviare messaggi, collegamenti Internet e anche file. Molti virus di nuova generazione usano programmi come Windows Live Messenger per diffondersi, contando così su un ulteriore vantaggio: i più evoluti, poi, usano dei software chiamati chatbot. Si tratta di programmi basati sul concetto di intelligenza artificiale, che analizzano i messaggi ricevuti e rispondono con delle domande pertinenti. Con un po' di fortuna, il software riesce a ingannare l'interlocutore e a convincerlo di parlare effettivamente con una persona in carne e ossa. Solo dopo aver scambiato qualche messaggio per confondere le acque, il chatbot si decide a invia re il file o il collegamento che contiene il virus.

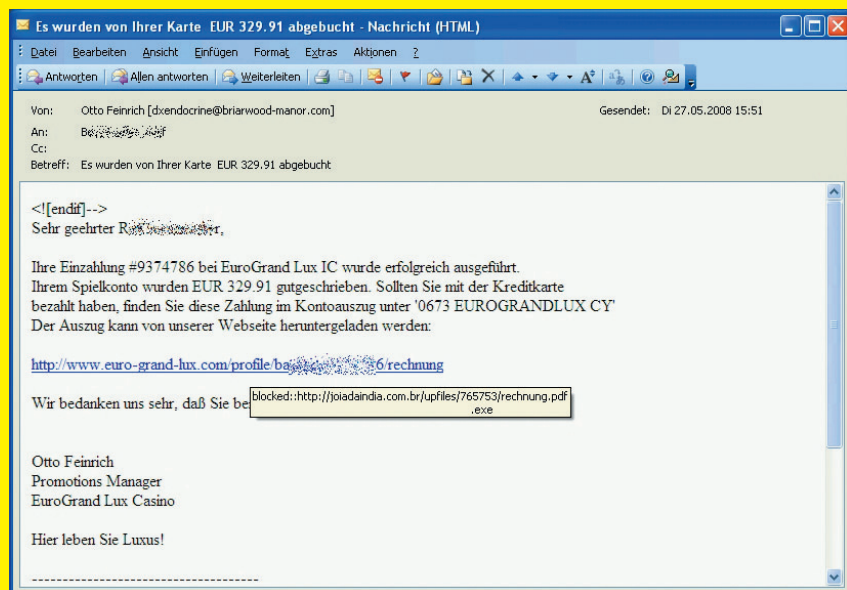
:: File Sharing

I sistemi P2P per lo scambio di file hanno sempre rappresentato un veicolo di diffusione per i virus. In questi ambiti, infatti, gli utenti cercano spesso file eseguibili o illegali, come i crack per programmi o videogiochi. Quando si ha a che fare con file del genere, il pericolo è sempre in agguato. La situazione, inoltre, è peggiorata negli ultimi anni. Un tempo, infatti,
i circuiti P2P erano frequentati solo da una nicchia di appassionati, che avevano un'approfondita conoscenza del PC e le idee molto chiare sui possibili pericoli che si annidavano in un circuito del genere. Oggi, invece, tra i partecipanti ci sono molti neofiti e persone che usano il computer occasionalmente e non si interessano più di tanto di ciò che succede "dietro le quinte". Si tratta delle vittime ideali per i pirati informatici, che hanno infatti intensificato l'uso del File Sharing come strumento per infettare nuovi computer. Secondo i dati raccolti dai laboratori GData, in un solo anno il numero di virus e spyware presenti nei circuiti P2P è aumentato del 60%.
Videogiochi online

Il boom dei videogiochi online, guidati dal capofila World of Warcraft, non ha mancato di suscitare l'interesse dei pirati informatici. Il livello di allerta, in questo caso, deve essere altissimo. In primo luogo, infatti, l'uso di un programma con un così stretto legame con il Web rappresenta un potenziale pericolo per la sicurezza. I principali sospettati sono i software aggiuntivi, sia che si tratti di cheat, ovvero di strumenti pensati per ottenere dei vantaggi nel gioco, sia che si tratti di semplici moduli aggiuntivi che offrono funzioni avanzate per arricchirne le funzioni.

Oltre a rappresentare un possibile veicolo di infezione, i giochi online sono essi stessi un bersaglio dei pirati informatici. Intorno ai videogame più celebri, infatti, si è sviluppato un vero "mercato nero" per la compravendita di oggetti, personaggi e account. Chi riesce a mettere le mani sui dati di accesso di un account di World of Warcraft, per esempio, può facilmente ricavarne centinaia o migliaia di euro, a seconda della "qualità" dell'account rubato.

ATTENTI AI COLLEGAMENTI

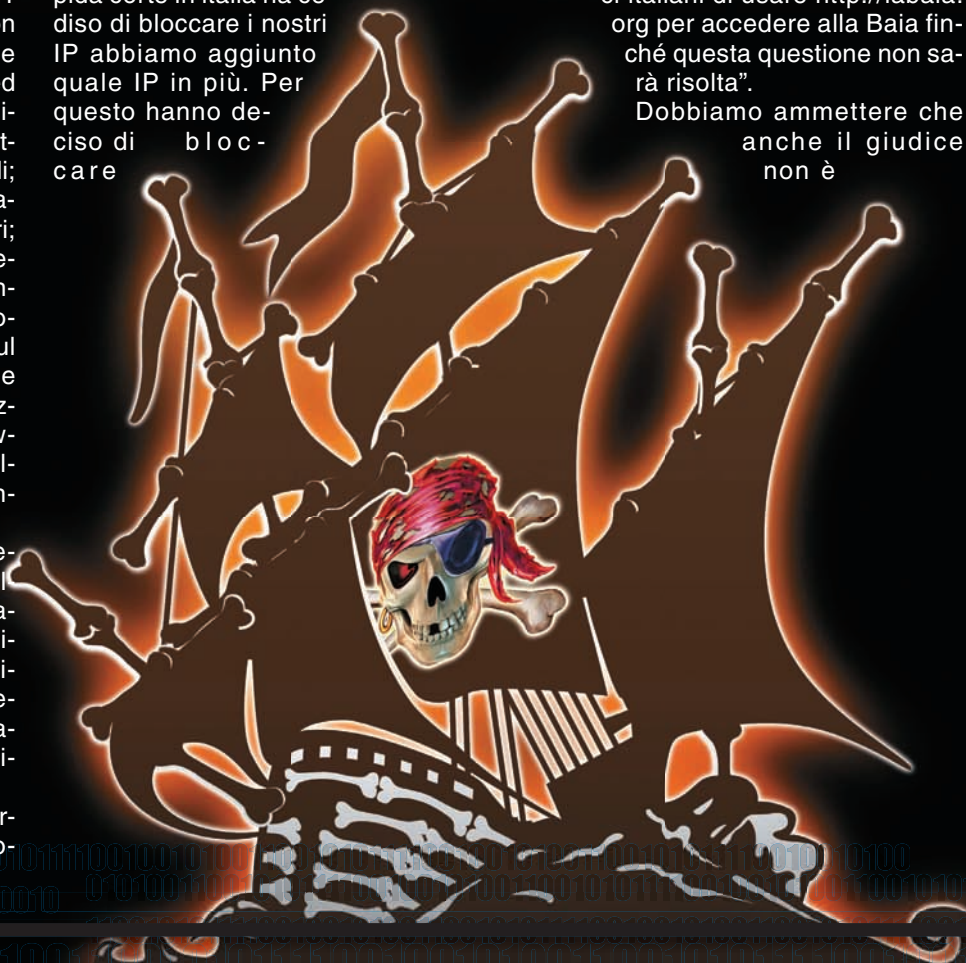
I virus allegati alle email hanno fatto il loro tempo. Ora i pirati usano un collegamento inserito nelle email. In questo caso, il messaggio è stato creato in modo da somigliare alla comunicazione di una compagnia telefonica tedesca e il collegamento dovrebbe consentire di scaricare la fattura della bolletta. Il nome del file è rechnung, ovvero "fattura". In realtà il file in questione non è un documento PDF, ma un eseguibile in formato EXE che contiene il virus. Per rendere ancora più difficile l'individuazione del pericoloso file, i pirati hanno usato una doppia estensione: rechnung.pdf.exe. Se scaricassimo il file con un computer impostato per nascondere le estensioni dei file, questo verrebbe visualizzato come rechnung.pdf e saremmo portati a credere che sia un innocuo documento.

ATTACCO ALLA BAIA

Un giudice italiano ha decretato il blocco agli accessi su thepiratebay.org e connessi, si preannuncia una vera e propria battaglia epica tra il tracker svedese e le corti italiane

"**...in ordine al reato previsto e punito dagli articoli 110 c.p. e 171 - ter, comma 2,** lettera a bis), della Legge 22 aprile 1941 n. 633 pochi in concorso tra loro e con altri attualmente ignoti, in violazione dell'articolo 16 della suddetta logge ed a fini di lucro, comunicavano al pubblico opere dell'ingegno protette dai diritto di autore, in particolare file musicali; documenti di testo; riproduzioni digitali di pubblicazioni a stampa; audiolibri; immagini; opere cinematografiche a televisive; programmi informatici (secondo il dettagliato elenco dinamico, in costante aggiornamento, pubblicato sul sito medesimo, distinto per tipologie di file, reperibile a partire dall'indirizzo web http://thepiratebay.org/browse), immettendo le opere stesse sulla rete Internet attraverso il sito identificato..."

Questo è il punto centrale del provvedimento preso dal Giudice dr. Raffaella Mascarino del Tribunale di Bergamo Sezione del Giudice per le Indagini Preliminari e della Udienza Preliminare su richiesta del Pubblico Ministero e con decreto si è stabilito l'oscuramento per tutti gli utenti italiani del sito thepiratebay.org e connessi.

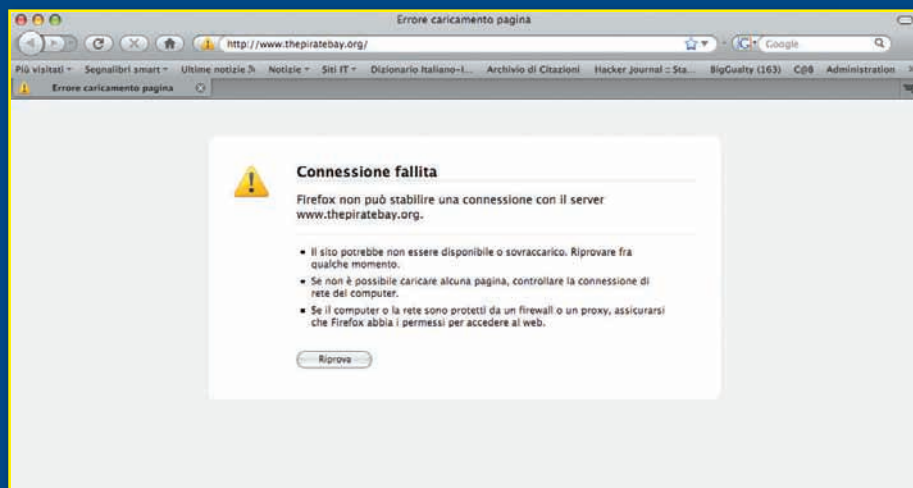
I ragazzi della Baia non si sono certo fatti prendere dallo sconforto e poche ore dopo già circolava per la rete una loro risposta che recitava letteralmente: "da quando qualche stupida corte in italia ha ceduso di bloccare i nostri IP abbiamo aggiunto quale IP in più. Per questo hanno deciso di bloccare il nostro DNS-name in Italia, e noi ne abbiamo aggiunto un altro. Fate girare la voce a tutti i vostri amici italiani di usare http://labaia.org per accedere alla Baia finché questa questione non sarà risolta".

Dobbiamo ammettere che anche il giudice non è

OPENDNS

Ecco in pochi passi come cambiare il proprio DNS in XP per poter navigare in tutti siti che vogliamo: <<<<immagini star_win da 1 a 6 seguendo gli step del tutorial>>>

1 - Entrate nel pannello di controllo.
2 - Andate nella vostra connessione di rete.
3 - Entrate nel pannello di controllo della LAN e poi su “proprietà”.
4 - Evidenziate il protocollo TCP/IP e cliccate su “proprietà”.
5 - Cambiate i DNS con i seguenti: 208.67.222.222 e 208.67.220.220
6 - Ora potete tranquillamente aprire tutti i siti che volete con il vostro browser.

stato con le mani in mano e tempo mezza giornata anche labaia.org era bloccato. Intanto abbiamo potuto assistere al solito balletto di IFPI e simili che hanno preso ad incensare l’opra del GIP di Bergamo, proprio sul sito dell’IFPI si può trovare una pagina (http://www.ifpi.org/content/section_news/20080812.html) di congratulazioni che rasenta il ridicolo: l’IFPI da il benvenuto all’azione della corte italiana contro The Pirate Bay.
Anche l’italianissima FIMI ha pensato bene di dire la sua nel sito (http://www.fimi.it/dett_comunicatistampa.php?id=113): “FIMI, federazione dell’industria musicale italiana, aderente a Confindustria, ha accolto con favore la decisione del GIP di Bergamo che ha imposto ai service provider italiani il blocco dell’accesso al sito pirate bay, noto per l’enorme quantità di materiale protetto da copyright messo a disposizione tramite le reti p2p.
“La magistratura ha mandato un segnale importante ai gestori del sito svedese che offriva migliaia di brani musicali di artisti, autori e produttori italiani con grave danno alla cultura del nostro Paese” ha dichiarato Enzo Mazza, presidente di FIMI.
“Le polemiche sulla presunta censura - ha concluso Mazza - sono strumentali e tendono a sviare l’opinione pubblica da un concetto fondamentale: pirate bay viola le norme penali italiane sulla proprietá intellettuale per questo era necessario bloccarlo ed indagare i titolari”.
L’ultima parola l’hanno avuta come al solito quelli di The Pirate Bay che hanno postato un messaggio sul loro blog (http://thepiratebay.org/blog) intitolato “Fascist state censors Pirate Bay” accusando il governo italiano di essere anti-democratico, di censurare la rete e portando alla luce anche delle riflessione su gli interessi persoanli/aziendali del premier Berlusconi nel contrastare il movimento del filesharing.
Tutti sanno come noi di HJ la pensiamo nei riguardi della questione P2P e libertà della rete, ripetiamo anche da sempre il nostro monito sull’utilizzo illecito della rete stessa. Nessuno mette in dubbio che tramite la Baia molti, moltissimi, scaricano film, musica, film e quant’altro andrebbe invece comprato pagando il diritto d’autore per chi quelle opere le ha pensate e realizzate, non c’è nessun dubbio sul fatto che un musicista abbia tutto il diritto a guadagnare sui brani che scrive e interpreta e questo vale anche per chi quel disco lo stampa e lo mette nei negozi e così pure per il negoziante stesso, torniamo, per la millesima volta, però a ripetere che se tutti questi personaggi, soprattutto etichette e distributori, rinunciassero a guadagni che rasentano la rapina, soprattutto rispetto a quanto guadagna l’artista, forse di dischi se ne venderebbero di più. Comunque tutto quanto fin qui detto e tutte le ragioni di chi difende il diritto d’autore non possono certamente giustificare la censura, nessuna forma di censura, e la libertà del web che deve anzi essere sempre più protetta visto che rimane l’unico medium ancora libero e accessibile a chiunque.
Finita la ramanzina vogliamo comunque dire a tutti che è possibile, in modo molto semplice, raggiungere la baia tramite l’utilizzo di proxy, tunneling e OpenDns, quindi buona navigazione a tutti.

BigG

Ecco cosa succede se provate a collegarvi a The Pirate Bay dopo il provvedimento del GIP di Bergamo

TUNNELING

Anche attraverso la pagina http://it.tunneling.net è possibile connettersi alla Baia utilizzando un proxy senza bisogno di installare nessun software sulla nostra macchina anche se tutti dovremmo averne almeno uno per la nostra navigazione anonima e sicura.

L'ATTACCO DEI CLONI

Falsi iPod, una console per videogiochi esteticamente simile al Wii ma con una tecnologia del secolo scorso, un telefono cellulare Nokia, l'n95, copiato prima ancora del suo ingresso in commercio in Europa... La contraffazione colpisce sia i marchi ad alta tecnologia, sia quelli di lusso

Il colpevole della creazione di questo mercato parallelo è talmente palese da rendere difficile il rispetto del principio della presunzione di innocenza. La Cina e la sua industria in piena espansione sembrano infatti al centro di questa vasta operazione. Quasi tutti gli esempi che siamo riusciti a scovare sono infatti prodotti nell'Impero di Mezzo, che non si preoccupa minimamente di copyright e licenze. I materiali assomigliano a quelli dei prodotti originali fino al punto da trarre in inganno chiunque e le copie sono esteticamente perfette; è sugli aspetti tecnici che si risparmia. Un falso iPod è in grado di leggere file MP3 ma non di collegarsi a un computer; la copia di un telefono cellulare d'avanguardia ci permette di chiamare un amico ma non offre funzioni Wi-Fi o Bluetooth o sostituisce il sensore fotografico da 2 MP con un obiettivo scadente, a malapena in grado di distinguere il giorno dalla notte.

Il 'pollo' di questo affare è sempre e comunque il consumatore; infatti, questi dispositivi, venduti su eBay o su siti che appaiono dal nulla per scomparire ancor più rapidamente, una volta acquistati non lasciano spazio ad alcuna possibilità di ricorso. Non è certo sufficiente pagare con una carta di credito assicurata per poter sperare in un risarcimento! Anche alcuni siti seri sono caduti nella trappola; è il caso di PriceMinister, che ha venduto un grosso lotto di falsi iPod credendo sinceramente di avere a che fare con un fornitore corretto...

L'unico consiglio utile per non farsi ingannare è quello di acquistare i prodotti tramite siti conosciuti, ai quali sia possibile rivolgersi in caso di problemi. Nel frattempo, diamo un'occhiata a questa guida, prestando attenzione a immagini e prezzi!

:: iPhone, clonazione in serie

MEIZU M8

L'iPhone di Apple sta beneficiando di un'enorme campagna mediatica mirata ai consumatori, che suscita un interesse altrettanto forte da parte di imprese non esattamente onestissime. L'esempio più eclatante è quello dell'azienda cinese Meizu, il cui stand al Cebit (il salone delle nuove tecnologie) di Hannover è stato sequestrato dalla polizia tedesca. Apple aveva infatti sporto denuncia contro Meizu per violazione delle norme sui brevetti e sulla contraffazione.

ONDA VX

L'azienda cinese Onda (niente a che vedere con la casa automobilistica Honda) offre un lettore MP3/MP4 il cui aspetto sembra 'casualmente' ispirato a quello di un telefono multimediale molto conosciuto in questo periodo.

HIPHONE

Mai sentito parlare dell'Hiphone? Beh, non ci permette di navigare sul Web... ma è davvero un problema? Il suo schermo tattile non è molto sensibile, è privo di memoria interna e si serve di un alloggiamento per

schede di memoria. D'altronde, a meno di 200 euro che cosa ci aspettavamo?

:: Wii: Nintendo non c'entra

CONSOLE TECHNIGAME01
Del Wii, la console più popolare del momento, esistono imitazioni dalle caratteristiche tecniche degne di una console Atari... dei primi anni '90. Vii (disponibile anche in versione Vii2), Technigame e altre hanno un solo vantaggio rispetto all'originale: il prezzo.
La Technigame costa meno di 40 euro e offre 16 videogiochi dal sapore 'nostalgico'. Per una Vii occorre invece sborsare circa 150 dollari.

:: L'iPod come prodotto di lusso

SAMSUNG SGH-X830
Il lettore SGH-X830 di Samsung presenta analogie che non sembrano casuali con l'iPod.
MP4-21
L'azienda cinese Shenzhen Sietek Industrial Co offre un lettore MP3/MP4 dall'aspetto molto simile a quello dell'iPod Nano di nuova generazione ed è entrato in commercio poco dopo l'originale.
MICROSOFT ZUNE
Ci si è messa anche Microsoft a fare concorrenza all'iPod di Apple. L'aspetto complessivo del dispositivo ricorda fortemente quello del prodotto fregiato dal logo della mela. Malgrado la tecnologia sia indiscutibilmente adeguata, il problema per Microsoft è che l'iPod rimane IL lettore portatile per eccellenza. Non rimane quindi che farsi ispirare...

:: Un Mac che non è un Mac

PSYSTAR OPENPC
Qualcuno doveva provarci e per il momento una sola azienda ha avuto il coraggio di farlo. Psystar commercializza negli USA (ma spedisce in tutto il mondo) un computer di nome OpenMac. Il dispositivo costa solo 400 dollari, contro gli oltre 2.400 euro del MacPro al quale intende fare concorrenza. L'OpenMac è venduto unitamente al sistema operativo Apple Leopard, il che è visto come il fumo degli occhi dalla casa con il logo della mela. Le prestazioni dei due computer non sono affatto paragonabili. L'OpenMac utilizza per esempio un processore AMD Core 2 Duo a 2,2 GHz, contro l'Intel dualcore a 2,8 GHz impiegato dal MacPro. L'elenco delle differenze potrebbe continuare a lungo; tuttavia, la possibilità di avere un Mac a meno di 400 euro fa certamente sognare...

:: Clonato il Nokia n95

NOKLA_N95
La risposta di Nokia all'iPhone di Apple si chiama n95. Questo telefono multifunzione è un piccolo gioiello della tecnologia che comprende tra l'altro un hard disk da 8 GB e un APN da 5 MP.

Venduto a meno di 450 euro (abbonamento escluso), ha dato vita a una miriade di cloni, come questo Nokla (con la 'l' al posto della 'i'), venduto in Cina (foto www.pcpop.com) a meno di 165 dollari, che offre le stesse funzioni sebbene in tono minore (l'APN è solo da 2 MP, per esempio).

:: Lettore Toshiba versione Made in China

SUNO MA917
Il lettore-ammiraglio di Toshiba, il Gigabeat, ha anche lui il suo clone, un prodotto cinese al 100% di nome Suno MA-917. ■

CLONE WARS
EPISODE II

Una chiacchierata col CAPITANO CRUNCH

Abbiamo parlato con uno dei miti dell'hacking e del phreaking invitato nel nostro paese per la manifestazione MOCA2008: ecco cosa ci ha rivelato su Wozniak, le blue box, la storica collaborazione con Apple e le ultime avventure tecnologiche

Gli albori del phreaking e la diffusione delle blue box? Lui c'era. Le riunioni del Homebrew Computer Club? Lui c'era. La nascita della Apple? Lui c'era. Il lancio del PC IBM: lui c'era. John Thomas Draper, meglio noto come Captain Crunch (http://www.webcrunchers.com/crunch/) è senza ombra di dubbio una delle figure chiave della storia dell'informatica e della telematica. Alla fine degli anni '60 apprese che inviando un suono a 2600 Hz era possibile effettuare telefonate interurbane attraverso la rete telefonica Statunitense e iniziò a creare congegni per generare questa frequenza, delle scatole note come "Blue box". In precedenza lo strumento ideale era un fischietto giocattolo che si trovava nelle scatole di cereali Cap'n Crunch e da questo personaggio Draper prese il suo leggendario soprannome muovendosi nel fertile ambiente del sud della California che si è poi trasformata nella Silicon Valley.

La prima celebrità ed i primi guai per le sue esplorazioni delle linee della Pac Bell Captain Crunch le deve ad un articolo di Esquire del '71, per colpa del quale finirà nel mirino delle autorità ma soprattutto venne contattato da un tale Steve Wozniak, ansioso di mostrargli la blue box che aveva costruito e capire come farla funzionare. Da qui è nata un'amicizia ed un rapporto anche professionale che dura ancora oggi, a distanza di più di 30 anni.

ESCLUSIVA

In questo lungo periodo Draper, con le sue gesta, la sua curiosità e caparbia indipendenza ha avuto a che fare con Apple, la IBM ed ispirato direttamente ed indirettamente generazioni di smanettoni in tutto il mondo ad esplorare i sistemi ed a piegarli a fare cose nuove e proibite.

Nel frattempo Captain Crunch non ha mai rinnegato le sue origini e le sue esperienze e non si è mai omologato o trasformato in un guru miliardario ma ha continuato a vivere a modo suo, spesso con pochi mezzi, ma sempre con tanta inventiva e entusiasmo. Lo stesso entusiasmo con cui in un caldo pomeriggio di agosto, invitato al campeggio tecnologico MOCA della Metro Olografix ci ha raccontato alcuni episodi del passato e aggiornato sulle sue ultime imprese.

Hacker Journal: Tu hai lavorato per Apple ad un'interfaccia telefonica per l'Apple II: com'è andata?

John Draper: Bisogna cominciare da come ho conosciuto Steve Wozniak. Mi contattò quando facevo il DJ in radio, alla KKUP e chiese se volevo venire a trovarlo e dare un'occhiata alla sua blue box. Voleva che mi spiegassi come usarla. Io ero molto sospettoso. Era un periodo in cui c'era un bust in corso, c'erano molti arresti e avevo paura che stessero cercando di incastrarmi. Così ho fatto in modo di andare a trovarlo senza avere con me nulla di compromettente e che non succedesse nulla di illegale. Quando sono arrivato Woz mi fece vedere la blue box che aveva costruito e non era un granché.
Il problema della sua blue box era che generava onde quadre invece che sinusoidali: in questo modo i toni non sono puliti. Sono di pessima qualità e chi l'avesse usata avrebbe generato una richiesta di assistenza in centrale perché non avrebbero accettato i toni.

Dopo essere diventati amici mi presentò Steve Jobs. Stava lavorando ad un computer a 6 bit al che io ho chiesto "Ehi, perché solo 6 bit?" Con 6 bit si è molto limitati e lui rispose che lo faceva "solo per provare che era in grado di creare un computer, ecco tutto". Poi qualche anno dopo lavorando rima alla Apple I e poi all'Apple II usò un cross-assembler fatto da me. Lo avevo fatto perché stavano arrivando sul mercato tutti questi microprocessori e c'era bisogno di assembler per sviluppare il software.

HJ: Quali microprocessori?
JD: Il cross-assembler era per l'[Intel] 8080, lo Z80, il 6502, il 1802 e il 6800. Lo feci su un sistema time-sharing system su cui c'era solo il Basic. Prendeva il codice assembler, ne faceva il parsing in opcode e poi l'output era in binhex (esadecimale) così che si poteva fare il dump su nastro.

HJ: Non si stampava?
JD: No, all'epoca per soli quindici dollari si poteva avere un lettore di nastri che venivano svenduti. E probabilmente lo stesso Gates inizialmente usò questo sistema in Microsoft attrezzandosi solo dopo con un sistema di sviluppo più robusto, chiamato Crust.

Wozniak stava lavorando all'Apple II e mi propose di progettare per loro una "charlie board" (http://www.webcrunchers.com/crunch/Play/comp_rev/charlie.html) [un'interfaccia per il telefono].

HJ: In Apple o come sviluppatore esterno?
JD: Esterno. Così realizzai la scheda con nove chip. E la reazione di Woz fu "Nove! Chip! No, merda, sono troppi!" e disse "Ho un progetto migliore" e me ne diede uno che impiegava solo cinque chip. Mi sono messo al lavoro su quello ma a un certo punto ho fatto a Woz "Ma stai usando una scheda a 6 bit invece di una a 8 bit" e lui "Eh sì, quelle a 8 bit costano troppo: posso farla a 6 bit e poi scrivere del software che fa in modo che devo comprare quei chip in più". Allora ho riflettuto su da dove tirar fuori i due bit mancanti e indovina cosa ho usato? La memoria, gli indirizzi di memoria. Facevo tutta una serie di peek e poke per far funzionare la scheda.

HJ: Ma è stata messa prodotta e messa in commercio?
JD: No. Ci ha pensato la AT&T a bloccarla. Erano spaventati.
Siccome tutto era in software, l'interfaccia poteva avere "fini malvagi" ed è chiaro che queste cose sono fuori discussione. Con il software giusto e una tabella dei toni la scheda si poteva trasformare in una blue box. AT&T non voleva nulla del genere. Fecero pressione su Jobs. Non su Woz, ma su Jobs perché dicesse "Accidenti, la AT&T dice che se facciamo uscire questa scheda ci faranno causa".

GLI SCHERZI

Il cofondatore di Apple Steve Wozniak è celebre per i suoi scherzi ed in particolare quelli telefonici (http://www.storiediapple.it/gli-scherzi-di-woz-telefono-che-passione.html) ma pochi sanno che ad ispirarlo è stato anche Captain Crunch con due gesta di phreaking entrate nella leggenda.
In una Draper riuscì da un telefono pubblico a fare una telefonata "circolare" facendo passare la chiamata attraverso centralini in vari paesi (tra cui Inghilterra, Russia e Giappone) fino a tornare negli Stati Uniti e far squillare il telefono nella cabina di fianco: alzando la cornetta si sentì, anche se flebile, la sua stessa voce dopo il giro (telefonico) del mondo.
Altra impresa fu quella di intercettare la parola segreta della CIA per le chiamate dirette al presidente Richard Nixon, subito sfruttata per chiamare il presidente e annunciare che c'era una crisi in corso. Alla sua domanda la risposta del Capitano fu "Siamo senza carta igienica, Signor Presidente."

Poi c'erano anche altri problemi. La scheda aveva bisogno di essere collegata alla presa del telefono e all'epoca, cioè nel 1975 o più probabilmente nel 1976, ci si poteva attaccare alla linea telefonica solo con un dispositivo di connessione approvato dalla Pac Bell. E il più economico costava 450 dollari.
Quindi per usare la scheda una persona doveva spendere anche questi ulteriori 450 dollari. Insomma, continuarono a fare pressione su Jobs del tipo "vi faremo causa".
Del resto non possono mica permettere che la gente colleghi le proprie cose alle loro linee telefoniche, giusto?

HJ: E poi che è successo?
JD: Poi è arrivato il modem della D.C. Hayes. Se ne uscirono con un modem a 1200 baud. Si poteva collegare alle loro linee telefoniche perché [la AT&T] in seguito ridussero un po' le restrizioni d'uso.

HJ: La scheda per Apple II che velocità avrebbe avuto?
JD: Circa 300 baud ma usavamo un phase shift, una modulazione programmabile. Era un anello ad aggancio di fase programmabile con cui individuare una frequenza e agganciarla. Il modem in pratica aveva un selettore di frequenze: l'avevo fatto via software.

HJ: Era una cosa diffusa trent'anni fa usare meno chip e fare tutto via software?
JD: Beh, era una specie di filosofia di Woz. A me non importava quanti chip avevo usato basta che tutto funzionasse. Wozniak invece ragionava più in termini di economicità.

HJ: Probabilmente dietro c'era Jobs.
JD: Proprio così. Jobs è stato influenzato molto da Woz, dal suo bisogno di fare le cose in economia. Era una cosa che Woz aveva, sai... perché Jobs lo manipolava. Jobs è fatto così. Oggigiorno [ad Apple] se entri in un ascensore e poi entra anche Jobs, nel tempo che arrivi al tuo piano puoi finire licenziato. È un tipo molto molto spietato.

HJ: Si dice che chieda "Cosa fai per me?"
JD: Proprio così: "cosa fai per me?". E se non gli dai una risposta giusta perdi il posto. Pessimo. Non si lavora bene con lui.

HJ: Quand'è l'ultima volta che ci hai avuto a che fare?
JD: L'ho incontrato quando sono stato alla Apple nei laboratori per fare dei test di un software.

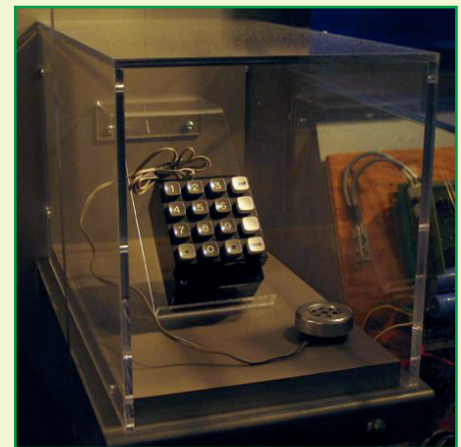
HJ: Quando è stato?
JD: Penso fosse nel 2004, 2005. Stavo lavorando su un software di VoIP per un'azienda.

HJ: Quindi dopo che la scheda per l'Apple II non è andata in porto ti sei dedicato a sviluppare il word processor EasyWriter (http://www.webcrunchers.com/crunch/stories/easywriter.html) per l'Apple II, giusto?
JD: È stato un po' dopo, due anni dopo. Ho sviluppato EasyWriter nel 1979. Barney Stone (www.stoneedge.com/about.htm) stava preparando un suo software fatto in Basic e io gli mostrai EasyWriter. Lui ne stava facendo uno in Integer Basic [il primo interprete Basic dell'Apple I e II, nda]

HJ: E il tuo?
JD: Il mio era scritto in Forth. E tutto il codice per lo scrolling era in assembly. Era molto veloce. Gli adattammo una VMI, una Virtual Machine Interface. Di questi tempi si userebbe il termine 'driver', video driver. Ne preparammo una per la scheda VIDEX.

HJ: Che cos'era?
JD: La Videx era una scheda di espansione video a 80 colonne per l'Apple II. In seguito facemmo la versione per il PC di IBM. FU necessario solo adattare il programma al video degli IBM.

HJ: Quindi ti sei dedicato al più remunerativo mercato IBM...
JD: Beh, sai, all'inizio quando uscirono i PC di IBM non erano così diffusi, c'erano in giro molti più Apple.

HJ: Cosa fai adesso?
JD: Lavoro per un'azienda chiamata En2go (http://www.en2go.com).

La mitica blue box di Crunch e Woz.

APPROFONDIMENTI

Per chi vuole capire meglio la figura del Capitano Crunch e il ruolo che ha avuto sin dagli anni '70 nella controcultura hacker sul suo sito ci sono tre preziose risorse.

Captain Crunch Phone Phreaking stories
http://www.webcrunchers.com/crunch/stories/

History of Hacking - videodocumentario di Discovery Channel
http://www.webcrunchers.com/crunch/video.html

Secrets of the Little Blue Box - lo storico articolo su Esquire
http://www.webcrunchers.com/crunch/stories/esq-art.html

Da un TG regionale ecco Captain Crunch mostrare al MOCA il sistema di distribuzione interattivo della En2go su cui lavora.

Ci occupiamo di distribuzione dei contenuti, di trasmettere video sul desktop degli utenti. Contenuti come film, intrattenimento, giochi, musica, animazioni 3D.
Sono il CTO della En2go, il responsabile tecnico in capo di cinque team software della che lavorano in ambiti specifici.

HJ: Vi occupare solo di software o anche di hardware?
JD: Software e hardware. In realtà al momento ci dedichiamo perlopiù al software ma abbiamo un dispositivo chiamato Flixo: è un sistema di distribuzione di video [in HD, nda] per Macintosh, per il desktop del Mac.

HJ: Solo per Macintosh?
JD: Stiamo lavorando anche su una versione per PC con Windows ma siamo ancora agli inizi.

HJ: Da questo deduco che usate i Mac.. Come mai?
JD: Per l'interfaccia e per Mac OS X. Sviluppiamo con Cocoa, l'ambiente di sviluppo Xcode. Cocoa è Objective C.

HJ: ...facilita il lavoro?
JD: Proprio così, è uno sballo. Uno sballo totale. Viene da NeXT. Il codice era di Jobs e se l'è portato in Apple. Ora è parte di Xcode e di Cocoa.

HJ: Avevi già usato NeXT Step?
JD: Sì, certo. L'ho usato quando uscì, è da lì che conosco Cocoa.

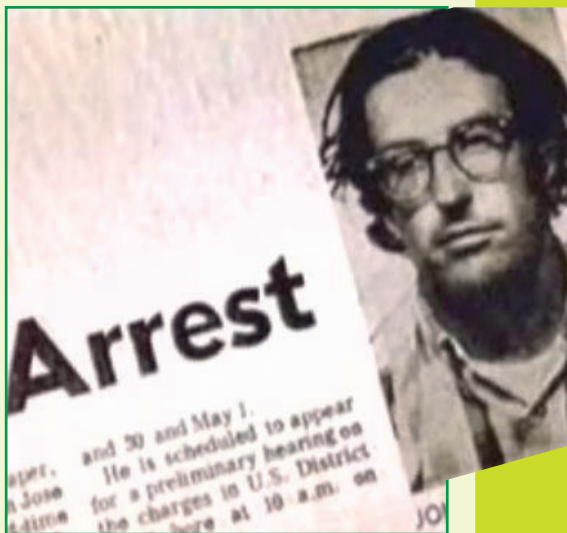
NdA: E per Windows?
JD: Lì usiamo, com'è che sia chiama... ah, Visual C++.

HJ: Oltre al lavoro hai qualche progetto personale?
JD: Progetti personali... ah, beh sì, sto facendo Crunch TV. È una serie di trasmissioni per uno dei canali di Flixo. Al momento si può trovare su www.crunchtv.net dove c'è il primo episodio da guardare come e quando si vuole.

HJ: E poi che cadenza avrà?
JD: Non è stato ancora deciso. Dovremmo spostare lo studio da Las Vegas a Hollywood. Abbiamo parecchio materiale già filmato ma è da montare. E non ho voglia di farlo io. Dovremo trovare qualcuno.

Si ringrazia la Metro Olografix (www.olografix.org) e Massimo "manray" Politi per le fotografie a John Draper.

Nicola D'Agostino

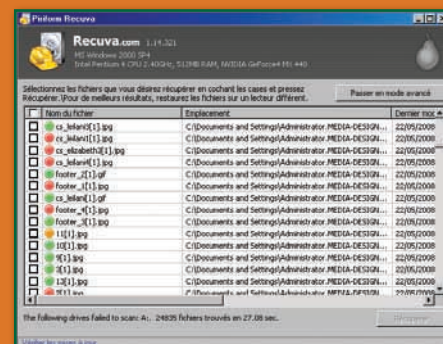
Arrest
and 30 and May 1.
He is scheduled to appear
for a preliminary hearing on
the charges in U.S. District
... at 10 a.m. on

L'annuncio dell'arresto di Captain Crunch.

Resuscitiamo i nostri file con RECUVA

Che sia sfortuna o sbadataggine, a tutti noi è capitato di eliminare per errore un file o una cartella indispensabili: foto, video, documenti di Word eccetera. Il programma di cui parliamo ci farà tirare un sospiro di sollievo...

Quando cancelliamo un file (dal cestino o direttamente da una scheda di memoria), questo non scompare completamente. Il sistema lo 'dimentica' ma non lo cancella fino a quando non viene registrato un altro file nella stessa posizione. Se abbiamo appena commesso l'errore, siamo ancora in tempo per porvi rimedio. La soluzione migliore è installare Recuva prima di trovarsi nelle condizioni di dover recuperare un file; non si sa mai, l'installazione potrebbe danneggiare il nostro prezioso file fotografico o video.

:: Un gioco da ragazzi

Dopo l'installazione, il wizard ci chiede di indicare quale tipo di file desideriamo recuperare (musica, documenti ecc.) e la sua ultima posizione conosciuta (Documenti, Cestino, scheda Flash ecc.). Infine, potremo scegliere l'opzione Analisi approfondita che permette di effettuare la ricerca in modo più preciso. Basterà quindi confermare la scelta e lasciare che il software faccia il suo lavoro. Al termine della scansione, Recuva indicherà i nomi dei file, la loro posizione e il loro stato. Un simbolo verde significa che il file è ancora in buone condizioni e può essere recuperato, mentre il simbolo arancione segnala la possibilità di un recupero parziale (nel caso di un video, sarà difficile ottenere un buon risultato). Per contro, un simbolo rosso indica che il recupero è impossibile, per esempio perché abbiamo atteso troppo tempo o abbiamo apportato troppe modifiche all'hard disk. Teniamo presente che Recuva consente anche di restaurare

file eliminati da bug, virus ed eventi accidentali. Se abbiamo perduto un file temporaneo di Microsoft Office (magari durante un blackout di corrente), Recuva potrà risolvere la situazione... ■

RECUVA

Dimensioni: 2246 KB
Licenza: Gratuita
Lingua: Inglese
Collegamento: www.recuva.com

OpenStreetMap

La cartografia vista dal basso

Ho un amico proprietario di una pizzeria. Se volesse stampare un volantino pubblicitario con una cartina per far sapere ai clienti dove si trova, avrebbe una sola possibilità per non commettere un reato fotocopiando il TuttoCittà o stampando la mappa di Google: disegnarsi la mappa a mano. Non tutti sono Caravaggio e, come il mio amico, quasi tutti ignorerebbero il problema. Anche TuttoCittà e Google non ci farebbero probabilmente troppo caso, ma di fatto avrebbe commesso un reato, esattamente come quando ci si copia un MP3. Nel 2004 è stato fondato da Steve Coast il progetto OpenStreetMap con l'obiettivo di creare, in spirito wiki, una cartografia libera dai vincoli del copyright. Pensare che persone qualsiasi possano arrivare a creare una cartografia paragonabile a quella commerciale sembra folle, ma di fatto è quello che è successo con GNU/Linux e con qualsiasi altro progetto FOSS che conosciamo. In Italia il progetto ha visto un'accelerazione nello sviluppo nell'autunno del 2006 quando chi scrive ha preso contatti con varie realtà legate ai GPS e tra queste con l'associazione GFOSS.it che ha creduto nel progetto e offerto il suo supporto alle attività. Disegnare una mappa potrebbe sembrare un processo complicato, che richiede competenze di CAD, di topografia, di misurazione, una cosa noiosissima direi. La realtà, invece, è molto diversa. Per partecipare al progetto non occorrono particolari competenze o apparecchiature, basta solo avere un po' di tempo a disposizione. Il possesso di un GPS non è un requisito fondamentale, anche se molto utile. È infatti possibile partecipare mappando semplicemente sulla base di foto satellitari o correggendo e integrando i dati già presenti. Anche le applicazioni utilizzate non richiedono particolari competenze o configurazioni del computer.

:: Diventare novelli cartografi

Ma come funziona, in pratica? Abbiamo detto che avere un GPS non è necessario, ma spiegheremo come si lavora avendone uno a disposizione. Chi non ne possiede uno può saltare semplicemente la fase di acquisizione dei dati sul campo e passare direttamente all'editing. Ammettiamo, comunque, di avere un GPS. Non è rilevante che si tratti di un navigatore da macchina, di un unità GPS professionale o di un palmare/telefonino collegato a un'antenna esterna. Quello che è importante, in realtà, è che sia possibile registrare i propri movimenti. Purtroppo non tutti i navigatori da macchina hanno questa funzione, per cui è consigliabile verificare nel menu del navigatore o verificare sul sito del produttore o su quello di OpenStreetMap. Uscite di casa, fate partire la registrazione e cominciate a camminare. Quando incontrate qualcosa che ritenete andrebbe inserito nella mappa (una farmacia, un distributore di benzina, una buca delle lettere...) prendete nota della posizione, del tipo di punto di interesse e dell'eventuale nome. La stessa cosa va fatta per le strade (nome, senso di marcia, limiti di velocità, eccetera). Una volta tornati a casa, procederete a scaricare dal GPS il tracciato del vostro giro e lo convertirete nel formato GPX (vedi box a lato). A questo punto occorre trasformare in mappa le informazioni che avete raccolto. Indipendentemente dall'applicazio-

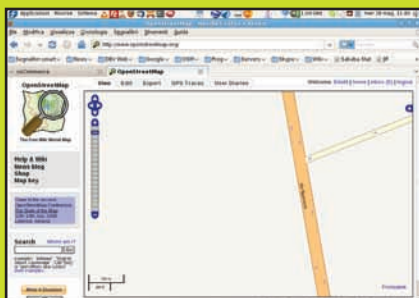
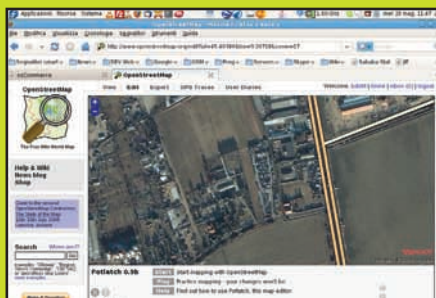
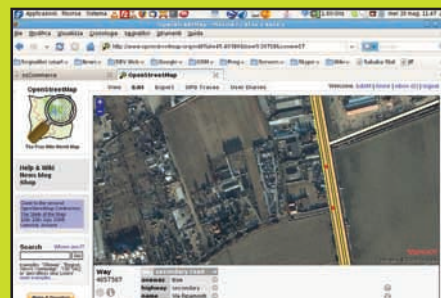
ne che userete per l'editing (ne parleremo più avanti) quello che vi troverete è una lunga serie di puntini che descrivono il precorso che avete fatto. Sulla base di questi disegnerete la mappa, semplicemente cliccando sul punto iniziale e tirando le righe che corrispondono alle strade. Poi a queste righe andrete ad attribuire le informazioni (nome, senso di marcia...). Finito questo passaggio probabilmente vorreste vedere i risultati sulla mappa. La mappa, però, non è aggiornata in tempo reale. Esistono infatti due rendering diversi che procedono in maniera distinta. Il principale (chiamato Mapnik) è quello che normalmente si vede visitando il sito del progetto OpenStreetMap. Viene aggiornato una volta a settimana, potrebbe quindi volerci qualche giorno prima che le vostre modifiche appaiano. Il secondo (chiamato Osmarender), invece viene aggiornato di continuo ed è possibile richiedere il ridisegno rapido di un'area. Normalmente la seconda mappa si aggiorna nell'arco di un paio d'ore se l'area modificata non è particolarmente complicata, e comunque entro la giornata se è molto densa di informazioni. Detta così sembra una cosa molto complicata, ma una mezz'ora di prove e due chiacchiere con altri contributori o nella mailing list italiana del progetto chiariscono tutti i punti oscuri e il processo diventa velocissimo e molto intuitivo.

:: Tool di disegno

In precedenza abbiamo anticipato qualcosa sull'esistenza di applicazioni per il disegno delle mappe. Ad oggi le due alternative principali (ma non sono le uniche) sono Potlatch e JOSM. Potlatch è un'applicazione scritta in ActionScript e si presenta come un'applet Flash all'interno del sito di OpenStreetMap. Ci si accede semplicemente cliccando sulla linguetta EDIT che appare in alto quando si consulta una mappa. È importante notare che questo editor, quando si avvia, chiede all'utente se questi abbia intenzione di lavorare sulla mappa o voglia solo fare un po' di pratica. È abbastanza ovvio che è consigliabile acquisire un minimo di familiarità con lo strumento prima di mettere mano a una mappa. L'uso è abbastanza intuitivo, ma qualora si volesse approfondire il suo funzionamento, la wiki del progetto ha una pagina dedicata (http://wiki.openstreetmap.org/index.php/It:Potlatch). JOSM è invece uno strumento molto potente: è scritto in Java (e quindi compatibile con qualsiasi ambiente), è ricco di plug-in ed è in continua evoluzione. Assomiglia vagamente a un ambiente di disegno CAD e al primo contatto può lasciare perplessi. L'interfaccia non è molto amichevole, ma già dopo pochi minuti se ne potrà apprezzare la potenza, la semplicità e la completezza. I due editor non sono necessariamente alternativi l'uno all'altro. Per la manipolazione di grosse aree o moli di dati è preferibile JOSM, ma per modifiche al volo è sicuramente più comodo Potlatch. JOSM, inoltre, grazie alla possibilità di essere espanso con plug-in, offre strumenti di verifica e risoluzione dei conflitti di editing.

:: L'evoluzione del progetto

Il progetto si è evoluto parecchio nel corso dell'ultimo anno, la base di dati è stata stravolta e oggi ha assunto una struttura decisamente stabile. Lo stesso strato di codice che definisce le API con cui le applicazioni si interfacciano al database è stata oggetto di un restyling lo scorso anno e prima dell'estate dovrebbe venire nuovamente aggiornato. Una grossa spinta al cambiamento è stato il dono, prime dell'estate 2007, della cartografia olandese, cinese e indiana da parte di Automotive Navigation

I SEI PASSI DEL MAPPATORE

1 Ecco un esempio di come aggiungere una strada in una mappa. Per prima cosa occorre identificare la zona in cui disegnare la mappa. Portatevi quindi allo zoom di 100 metri e cliccate sulla linguetta Edit in alto, dopo esservi loggati.

2 Dopo il login l'editor Flash si attiverà. Se nella zona scelta esistono immagini satellitari di buona risoluzione, appariranno come sfondo. La prima scelta sarà se fare pratica (Play) o disegnare davvero (Start). Le prime volte, ovviamente, è meglio fare pratica.

3 Cliccate su una strada esistente per selezionarla. Posizionatevi sul punto in cui far partire la nuova strada e create un punto di partenza sulla mappa con la combinazione Shift+Click. Vedrete il punto apparire sullo schermo.

Data, un'omologa olandese di NavTeq e TeleAtlas. La necessità di integrare questi dati (e in seguito anche quelli del dataset TIGER statunitensi) ha portato alla luce alcune incongruenze e rigidità della struttura precedente che è stata quindi manipolata introducendo nuovi paradigmi ed eliminando strutture di dati ridondanti. La filosofia di collaborazione in stile wiki del progetto comporta un'estrema flessibilità nel tipo di dati che possono essere inseriti nel database. Di fatto chiunque può inserire qualsiasi tipo di informazione. Esiste, ovviamente, un set di informazioni e uno standard di inserimento delle stesse che è condiviso, elaborato tramite discussioni e votazioni, ma, in fondo, si tratta essenzialmente di linee guida o consigli. Definire invece un metro per indicare la completezza di un progetto del genere è decisamente complicato. È completa una mappa che ha tutto il reticolo stradale sistemato o quella che riporta tutte le banche, le farmacia, le buche delle lettere e i bagni pubblici? Dire che un'area è completa sarebbe falso perché si limiterebbe a riconoscere la presenza di tutti i punti di interesse "comuni" ma potrebbe non esserlo rispetto a quelli "particolari".
Quello che possiamo comunque dire è che, al di là di nazioni come il Regno Unito, l'Olanda e gli Stati Uniti - dove il progetto è partito da qualche anno o dove è stata importata una grossa mole di dati da archivi esterni – la copertura è nel caso migliore a macchia di leopardo (Germania). In Italia la copertura si sta estendendo sempre più, ma c'è ancora molto da fare. Non mancano, ad ogni modo, esempi dove le mappe di OpenStreetMap sono non solo più complete o precise, ma talvolta anche le uniche disponibili. Un caso eclatante in questo senso è l'Isola di Man, famosa per la corsa del Tourist Trophy che ogni anno coinvolge centinaia di motociclisti. Di fatto l'unica mappa disponibile online dell'isola è quella di OpenStreetMap.

:: La struttura tecnica

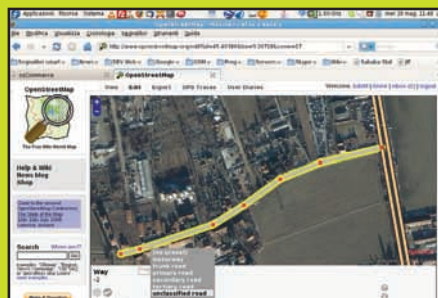
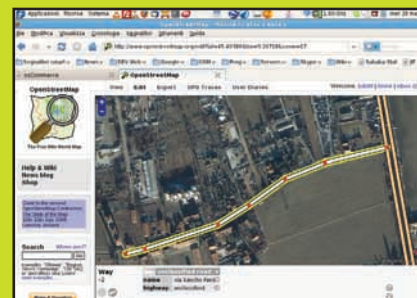
Il successo del progetto si misura anche con l'evoluzione dell'infrastruttura che lo tiene in piedi. Dai due server di recupero degli inizi, si è arrivati oggi ad una struttura più complessa, forse ancora sottodimensionata e migliorabile, ma sicuramente adatta allo scopo. È possibile avere una fotografia aggiornata consultando la pagina Server del wiki di OpenStreetMap, ma possiamo semplificare dicendo che

- il database ad oggi è basato su MySQL, ma si sta indagando la possibilità di portarlo su PostGIS per sfruttarne le funzioni legate al mondo GIS;
- esiste un file server che mantiene le immagini delle singole mattonelle che compongono la mappa;
- un server Web ospita le API.

A questo si affianca un ulteriore server che tramite virtual machine ospita il wiki, il sistema trac e il server subversion.

LINKOGRAFIA

- www.openstreetmap.org - Il sito del progetto OpenStreetMap.
- http://wiki.openstreetmap.org/index.php/WikiProject_Italy - Il progetto Italia che ha lo scopo di raccogliere e coordinare gli sforzi per la realizzazione della cartografia italiana all'interno del progetto OpenStreetMap.
- http://osmitalia.splinder.com - Il blog degli utenti italiani di OSM.
- www.gfoss.it - Il sito della comunità italiana degli utenti e sviluppatori di software geografico libero e a codice sorgente aperto.

4 Cliccate nuovamente sul punto (verrà selezionato solo lui) e facendo nuovamente Shift+Click inizierete il disegno di una nuova strada. Cliccate sui punti in cui questa strada curva e terminate con Invio. Non esagerare con il numero di punti.

5 A questo punto la strada è selezionata e dovete definirne la tipologia. Per le strade cittadine o non di scorrimento veloce va benissimo unclassified. Per strade statali è meglio usare, invece, primary e per le autostrade motorway.

6 Assegnate un nome alla strada e cliccate in un altro punto dell'immagine in modo da deselezionare la strada. Dopo qualche istante il numero negativo in basso a sinistra cambierà, indicando che la strada è stata caricata con successo nel database.